Towards Highly Interactive Honeypots for Industrial Control Systems
Stephan Lau, Johannes Klick, Stephan Arndt and Volker Roth
<firstname>.<surname>@fu-berlin.de

Internet-facing Siemens PLCs

About 3700 Siemens S7 PLCs are connected to the Internet, at least 230 honeypots can be trivially identified. Adversaries are likely aware of their existence and may perform a thorough inspection to avoid them. We should improve ICS honeypots regarding their interactivity in order to use them effectively.

Honeypot Classification in the ICS World

Unlike usual honeypots, which only emulate a specific software, Industrial Control Systems are general computing devices. They allow interaction with the system and its loaded program separately. We extended the traditional honeypot classification to account for that:

Low-interactive
The adversary can interact with the host only.

Medium-interactive
The adversary can interact with the host and the program.

High-interactive
The adversary can additionally read and write programs.

The First High-interactive ICS Honeypot

XPOT is the first high-interactive PLC honeypot and can be used to distract and analyze advanced adversaries. Since it is software-based, it is very scalable and enables large decoy or sensor networks. XPOT can be connected to a simulated industrial process in order to make adversaries’ experiences comprehensive.

XPOT – A Programmable PLC Honeypot

We developed XPOT, a software-based high-interactive PLC honeypot which can run programs. It simulates a Siemens S7-314C-2 PN/DP.

- modifiable memory areas
- debuggable with monitor mode
- programmable with common IDEs
- executes program, supports compilation and interpretation
- spoofed TCP/IP stack, mimics OS fingerprint and quirks

Features and Classification of ICS Honeypots

<table>
<thead>
<tr>
<th>TCP/IP stack spoofing</th>
<th>read System State List</th>
<th>HTTP SNMP</th>
<th>list blocks</th>
<th>read memory</th>
<th>write memory</th>
<th>start/stop CPU</th>
<th>up-/download blocks</th>
<th>execute program</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conpot</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
<td></td>
</tr>
<tr>
<td>Snap7</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
<td></td>
</tr>
<tr>
<td>CryPLH2</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
</tr>
<tr>
<td>XPOT</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
<td>(✓)</td>
</tr>
</tbody>
</table>